UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,832	07/21/2000	Raynold M. Kahn	PD-200055	4474

20991 7590 09/11/2003

HUGHES ELECTRONICS CORPORATION
PATENT DOCKET ADMINISTRATION
BLDG 001 M/S A109
P O BOX 956
EL SEGUNDO, CA 902450956

EXAMINER	
DEMICCO, MATTHEW R	
ART UNIT	PAPER NUMBER
2697	

DATE MAILED: 09/11/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/620,832	KAHN ET AL.	
	Examiner	Art Unit	
	Matthew R Demicco	2697	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 July 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4,5,6,7* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: Figure 1, 116; Figure 2, 212; Figure 4, 420; Figure 5, 526. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. The specification is objected to for the following reason: the Examiner requests that Applicant update the copending application data to include appropriate serial numbers.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 16-24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The current invention is a video recording device with multiple layers of encryption for recorded content and encryption keys.

Regarding Claim 16, Applicant claims an apparatus comprising a fourth decryption module. The Examiner cannot find any support for the claimed fourth decryption module in the specification or drawings.

Regarding Claim 17, Applicant claims the apparatus of Claim 16 further comprising a second media storage device, a third encryption module, a fourth decryption module and a fifth decryption module, communicatively coupled to the second media storage device. The Examiner cannot find any support for the claimed second media storage device, third encryption module or forth and fifth decryption module in the specification or drawings.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-16 and 20-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,266,481 to Lee et al. in view of U.S. Patent No. 5,761,302 to Park.

Regarding Claim 1, Lee discloses a method of storing program material for subsequent replay (Col. 2, Lines 18-20) comprising the steps of receiving access control information (Col. 4, Lines 15-30) and the program material encrypted (Col. 8, Lines 25-

28) according to a first encryption key (See Figure 3, "Ks" and Col. 8, Lines 29-38), the access control information including the first encryption key and control data which are multiplexed with the television programs (Col. 8, Line 2). Further disclosed is encrypting the access control information according to a second encryption key (See Figure 3, "Kw" and Cols. 8-9, Lines 65-8). Additionally disclosed is encrypting the second encryption key according to a third encryption key to produce a forth encryption key (See Figure 3, "Kp" and Col. 9, Lines 40-43) and storing the encrypted access control information, program material (Col. 9, Lines 22-26), and fourth encryption key (Col. 9, Lines 45-48). While Lee discloses a method of transmitting and storing program data and control information in a very secure way using multiple levels of encryption to protect data, what is not disclosed, however, is a method wherein the program material is stored in an encrypted form once received by an authorized user. Park discloses a digital video method of copy protection using transmitted and recorded encrypted key information (Col. 2, Lines 40-45) wherein video to be recorded locally is encrypted (See Figure 5, Steps 7 and 8). Park is evidence that ordinary workers in the art would appreciate the use of encryption to copy-protect video information on a user's storage device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the multiple encryption video distribution and recording method of Lee with the encryption of recorded data of Park in order to add an even higher level of copy protection to a personal video recorder.

Regarding Claim 2, Lee in view of Park disclose a method as stated above in Claim 1. Further, Lee discloses reading the encrypted access control information,

program material and the fourth encryption key, decrypting the encrypted access control information to produce the encrypted access control information, decrypting the fourth encryption key using the third encryption key to produce the second encryption key, decrypting the encrypted access control information to produce the first encryption key, and decrypting the program material using the first encryption key (See Figure 3, Elements 38, 39, and 35 and Cols. 11-12, Lines 43-3).

Regarding Claim 3, Lee in view of Park disclose a method as stated above in Claim 2. Lee further discloses a method wherein the access control information further comprises data describing a right associated with the program material (Col. 4, Lines 15-30) and the steps of decrypting the encrypted access control information to produce the first encryption key and decrypting the program material using the first encryption key is performed according to the data describing the right (Col. 9, Lines 49-60).

Regarding Claim 4, Lee in view of Park disclose a method as stated above in Claim 3. Park further discloses that the access control information may be multiplexed and transmitted in the same channel as the video programming as stated above. This table of multiplexed access information reads on the claimed metadata table.

Regarding Claim 5, Lee in view of Park disclose a method as stated above in Claim 4. Lee further discloses that the metadata table comprises at least one control value expressing a condition (Col. 4, Lines 15-30) that must be satisfied before pre-cached program material (See Figure 4, 45) is presented to the subscriber (Col. 11, Lines 55-50).

Regarding Claim 6, Lee in view of Park disclose a method as stated above in Claim 3. Lee further discloses that the right is a viewing right having a lifetime of program material after a purchase of the program material (Col. 4, Lines 24-27).

Regarding Claim 7, Lee in view of Park disclose a method as stated above in Claim 2. Lee further discloses providing the program material to a presentation device (Col. 12, Lines 1-3).

Regarding Claim 8, Lee in view of Park disclose a method as stated above in Claim 2. Lee discloses storing the decrypted program material (Col. 8, Lines 49-50) and reading the program material according to a user command (Col. 12, Lines 1-3).

Regarding Claim 9, Lee in view of Park disclose a method as stated above in Claim 8. Lee further discloses a user command is a trick-play command such as fast forward (Col. 6, Lines 38-56). It is further inherent in such a digital VCR that other functions such as play, rewind, pause, and stop are available to the user.

Regarding Claim 10, Lee in view of Park disclose a method as stated above in Claim 2. In the method of Lee, it is necessary to decrypt the program data and control information fully in order to display it to the user. Lee further discloses storing the program data on a digital VCR. Park discloses storing the program data in an encrypted form as stated above. Therefore, the method of Lee in view of Park as disclosed above would necessarily re-encrypt the decrypted program material that is viewed by a user, for storage purposes. Using the multiple encryption method of Lee, this would entail encrypting the second encryption key according to a third encryption key to produce a

fourth encryption key, and storing the program material and fourth encryption key as stated above.

Regarding Claim 11, refer to Claim 3 above.

Regarding Claim 12, Lee in view of Park disclose a method as stated above in Claim 11. In order to play from storage the re-encrypted program material, it is necessary to read the re-encrypted program material and fourth encryption key, decrypt the fourth encryption key with the third key to produce a second encryption key, and decrypting the program material using the second encryption key as stated above in Claim 2.

Regarding Claim 13-15, refer to Claims 7-9, respectively.

Regarding Claim 16, as best understood by the Examiner, Lee in view of Park disclose an apparatus for storing program material for subsequent replay as stated above. Lee further discloses a tuner (Col. 4, Line 49) for receiving encrypted access control information and program materiel encrypted according to a first encryption key (See Figure 4, "Km"), the access control information including the first encryption key and control data as stated above in Claim 1. Lee further discloses a first encryption module (41), communicatively coupled (See Figure 4, "High Speed Data") to the tuner and to a data storage device (45), the first encryption module for further encrypting the encrypted program material and access control information according to a second encryption key (Km) as stated above. Lee further discloses a second encryption module (30), communicatively coupled to the first encryption module (41) for encrypting the second encryption key according to a third encryption key (Kw) to produce a fourth encryption key as stated above. Lee also discloses a first and second decryption module as stated

above in Claim 2. Also disclosed is a conditional access module (Col. 5, Lines 41-51), communicatively coupled to the second decryption module (44) and tuner (See Figure 4, 33) for selectable accepting the access control information selected from the group comprising the access control information received in the tuner and the access control information decrypted by the second decryption module as stated above. Further disclosed is a third decryption module (39) for decrypting the encrypted access control information to produce the first encryption key (Ks) as stated above. This module is communicatively coupled to the CPU of the invention of Lee (See Figure 4, 35) via a data bus, and it is well known in the art that the modules may be implemented together. This reads on the claimed conditional access module comprising the third decryption module. Lee also discloses a fourth decryption module (35) for decrypting the encrypted program material to produce unencrypted program material using the first encryption key (Ks).

Regarding Claim 20, as best understood by the Examiner, Lee in view of Park disclose an apparatus as stated above in Claim 16. Lee further discloses a fourth decryption module (35) in communicatively coupled to the first encryption module (41) through the aforementioned high-speed data connection. Further, the second decryption module (44) is communicatively couple-able to a presentation device (14).

Regarding Claim 21, as best understood by the Examiner, Lee in view of Park disclose an apparatus as stated above in Claim 20 wherein the first encryption module (41) encrypts the unencrypted program material ("Data In") using the second encryption key (Km) and the second decryption module (44) accepts the encrypted program material

from the data storage device (45) and decrypts the encrypted program material using the second encryption key (Km).

Regarding Claim 22, as best understood by the Examiner, Lee in view of Park disclose an apparatus as stated above in Claim 16. Lee further discloses an apparatus comprising the data storage device (45) for storing and retrieving the further encrypted program materials and the forth enecryption key as stated above.

Regarding Claim 23, as best understood by the Examiner, Lee in view of Park disclose an apparatus as stated above in Claim 16. Lee further discloses an apparatus wherein the decryption module may be implemented on a smart card (Col. 6, Lines 1-12). This reads on the claimed third decryption module being implemented on a smart card.

Regarding Claim 24, as best understood by the Examiner, Lee in view of Park disclose an apparatus as stated above in Claim 16. Lee further discloses an apparatus wherein the control data contains information related to an expiration period (Col. 4, Lines 15-30). Since the expiration period varies with time, the control data inherently contains information that is temporally variant.

Regarding Claim 25, Lee in view of Park disclose an apparatus for storing program material for subsequent replay as stated above. Further disclosed are means for receiving access control information and program material encrypted according to a first encryption key, the access control information including the first encryption key and control data as stated above in Claim 1. Further disclosed are means for further encrypting the access control information and encrypted program material according to a second key, means for encrypting the second encryption key according to a third

encryption key to produce a fourth key and storing the information, program material and fourth key as stated above in Claim 1.

Regarding Claims 26-27 and 28-37 refer to Claims 2-3 and 6-15 above, respectively.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent No. 4,613,901 to Gilhousen et al. discloses a system of scambling and descrambling television signals using a DES key.

b. U.S. Patent No. 6,466,921 to Cordery et al. discloses a data transfer system using DES encryption and encrypting the encrypting key for additional security.

c. U.S. Patent No. 6,456,985 to Ohtsuka discloses a system for encrypting image data wherein the encryption key is further encrypted for additional security.

d. U.S. Patent No. 6,516,465 to Paskins discloses a digital video receiver with conditional access module using encrypted messages.

e. U.S. Patent No. 6,055,314 to Spies et al. discloses a system for secure purchase of video content using a smart card and encryption.

f. U.S. Patent No. 5,715,403 to Stefik discloses a system for distribution of digital media with metadata access information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew R Demicco whose telephone number is (703) 305-8155. The examiner can normally be reached on Mon-Fri, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Faile can be reached on (703) 305-4380. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-0377.

mrd
September 3, 2003

CHRIS GRANT
PRIMARY EXAMINER